

SLK Fueling and Distributing
Canville, Washington



Facility Security Plan

- SENSITIVE SECURITY INFORMATION

BUSINESS CONFIDENTIAL

Disclaimer: This example manual is based in the interim final rule for 33 CFR 105 and as is offered as a learning tool. This plan is not a complete document and has not been reviewed for compliance with the regulations. Unfortunately the review process is in development at this point and could not be used as a training tool.

“WARNING: THIS DOCUMENT CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER THE PROVISIONS OF 49 CFR PART 1520. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION. FOR US GOVERNMENT AGENCIES, PUBLIC AVAILABILITY TO BE DETERMINED UNDER 5 U.S.C. 552.”

Facility Security Plan//Sensitive Security Information

COMPANY PROFILE

Date: 01 December 2003

Company Name: SLK Fueling and Distributing

Company Address: 123 Somewhere Street

Company Address: Canville, WA 98000

Facility Location: SLK is physically located on the coast of Washington in Howeird Bay, a tributary waterway to the Pacific Ocean. The facility is 20 miles from Canville, WA. The facility has a railroad spur, truck and vessel stations.

General Manager: J. R. Doe

Office: 206-444-1212//Home:206-444-1313

Please contact only after trying and failing to contact the Mr. Font or Mr. Fontsans.

Primary POC: Tempus Font

Title: Facility Security Officer

E-mail: tfont@maybe.com

Office: 206-555-1212

Home: 206-555-1212

Cell: 253-555-1212

Secondary POC: Serif Fontsans

Title: Assistant Security Officer

E-mail: sfontsans@maybe.com

Office: 206-555-1212

Home: 206-555-1212

Cell: 253-555-1212

Plan Completed By: MR TEMPUS FONT HAS BEEN DESIGNATED THE FACILITY SECURITY OFFICER AS DEFINED IN 33 CFR105. AS SUCH HE IS RESPONSIBLE FOR THE CONTENTS AND ACCURACY OF THIS PLAN. HE HAS BEEN GIVEN THE AUTHORITY TO PROCEED WITH ACTIONS IN ACCORDANCE WITH THIS PLAN ONCE APPROVED BY THE COGNIZANT COTP.

Facility Security Plan//Sensitive Security Information

TABLE OF CONTENTS

- 1. Security administration and organization**
- 2. Personnel Training**
- 3. Drills and Exercises**
- 4. Records and Documentation**
- 5. Response to Change in MARSEC Level**
- 6. Procedures for interfacing with vessels**
- 7. Declaration of Security (DOS)**
- 8. Communications**
- 9. Security systems and equipment maintenance**
- 10. Security measures for access control, including designated public access areas**
- 11. Security measures for restricted areas**
- 12. Security measures for handling cargo**
- 13. Security measures for delivery of vessel stores and bunkers**
- 14. Security measures for monitoring**
- 15. Security incident procedures**
- 16. Audits and security plan amendments**
- 17. Facility Security Assessment (FSA) report**
- 18. Facility Vulnerability and Security Measures Summary**

Section 1. Security Administration/Organization

A quick reference card with useful administrative information has been placed at the beginning of the manual. Please refer to it for contact names and numbers useful in this plan.

A. Useful definitions used in this Plan–

- **MARSEC** - Is the Acronym for Maritime Security. This is used in a level system to indicate the current perceived threat to the marine elements of the national transportation system.
- **MARSEC I** – The degree of security precautions to take when the threat of an unlawful act against a vessel or terminal is, though possible, not likely. Minimum protective measures shall be maintained.
- **MARSEC II** – The degree of security precautions to take when the threat of an unlawful act against a vessel or terminal is possible and intelligence indicates that terrorists are likely to be active within a specific area, or against a type of vessel or terminal.
- **MARSEC III** - The degree of security precautions to take when the threat of an unlawful act against a vessel or terminal is probable or imminent and intelligence indicates that terrorists have chosen specific targets.
- **Declaration of Security (DoS)** is an agreement between the responsible Vessel and Facility Security Officers that provides a means for ensuring that all shared security concerns are addressed and security will remain in place throughout the time that a vessel is moored to the facility.
- **Definitions of elements required by the MTSA** implementing regulations are found in 33 CFR 101.105. Please refer to these regs or ask the FSO for help if there are questions with the contents of the manual.
- **The Daylog** is an electronic document that keeps track of daily security business. Items to enter are: watch relief, visitor names, names of watch standards, findings of patrols, vessels moored, gates open and why, and anything that impacts security, like changes of MARSEC status. The Daylog is a record of twelve hours.
- **Vulnerability Assessment** is the process included in the interim final rule (33 CFR 105) wherein the Facility Security Officer will use available technologies and information to discover the threats to her/his facility; examine existing security measures and equipment; and evaluate methods for providing protection from reasonable security threats. (see Section 17)

B. Sensitive Security Information:

Includes all information specifically mentioned in 49 CFR 1520 including port, facility, and vessel security plans. Much of this plan deals with information that is not suitable for release to the general public. This is information that, if compromised, may jeopardize the security of a transportation system. Establishing certain safeguarding measures is necessary to prevent unwanted disclosure of such information to those who pose a threat to Maritime Transportation System. The Captain Of The Port will strictly control this category of information in accordance with 49 CFR 1520, regardless of the medium in which it is transmitted. Recipients with access to the portions of

Facility Security Plan//Sensitive Security Information

this plan that contain SSI are considered end-users and must comply with the handling procedures prescribed in this section. For additional specific information not included in this plan regarding the handling, storing or transmission of SSI information, please contact the security manager at the cognizant Coast Guard Office.

When an individual takes custody of SSI information, it is the responsibility of that individual to safeguard the document at all times and ensure that positive measures are in effect to restrict access to the container (limited distribution of keys and/or combination). When SSI information is left unattended it shall be in a locked container or office or otherwise stored out of view of unauthorized personnel.

It is the responsibility of the document holder to ensure that the SSI document is appropriately marked and packaged to ensure that the enclosed information is not compromised. The document shall be packaged in opaque envelopes with an attention line used to identify the specific recipient of the information. If hand-carried, the document should be appropriately marked and then covered with an opaque cover sheet to prevent visual compromise

The intent of SSI destruction is to prevent the recovery of the document by a third party. Any method prescribed for the handling of national security classified material is authorized; however, if manual destruction is necessary the document may be cut or shred into pieces not larger than ½” per side.

C. Security Organization

Background: Our facility, SLK Fueling and Distributing has multiple contact points through which threats can occur. There are docks for deep draft vessels, barges and fishing vessels up to fifty feet in length. There is a transfer station for tanker trucks and for rail cars. John Doe Incorporated in Chicago is the owner of the facility and J. Doe Limited, 123 Somewhere Street, Canville, WA 98000 is the operator. The facility receives diesel and slops from ships, diesel and bunker fuel from barges and lube oils from trucks. The facility delivers diesel to tank trucks and fishing boats. Lube oil is delivered to ships and fishing boats and bunker fuel is delivered to ships. The slops are transferred to a train car and delivered for recycling to Canville.

Security Officer: The facility has the following personnel at the top position of the Security Chain of Command:

- I. J. R. Doe jr //Company President—Security Trained//ICS-300
- II. Tempus Font//Facility Security Officer---Security Trained//ICS-300
- III. Serif Fontsans//Assistant Security Officer---Security Trained//ICS-200

Patrol Team One is made up of personnel who have been trained to minimum-security standards, they are personnel accepted by the Facility Management to represent the Facility as Guards, Security Watch standers and Station Watch Standers.

Patrol Team One is the group who is put on duty when a ship has tied up at the dock, the following facility personnel have received the training to be part of Patrol Team One:

(the first eight names are full time security)

Bob McNab

Shelly Bere

Willy Mare

Niu Kim

Facility Security Plan//Sensitive Security Information

Bien Muir	Vari Zigong	Hi N. Lois	Andrew Cap
Lucy Vandpelt	George Washington	Abe Linkin	Badrei Nimia
Kaber McNulty	Vorse Birson	Corky Amand	Reggie Smith
Karla Jones	Chip Rogers		

Our facility requires that Patrol Team One be made up of two persons at the lowest level of security and this number shall be augmented as required to a maximum of five persons. If more than five personnel are required, additional security personnel shall be hired from outside sources for perimeter surveillance and such duties. Local Companies: A1 Security, LoneStar and Belcamp Private Security all have personnel trained to the appropriate level.

D. Watch Routine

A minimum of two personnel will share a watch, on MARSEC I. These personnel are part of Patrol Team One. A watch interval is 12 hours. This time is divided so that each guard will get a two hour rest period. Rotation is designed with input from the full time guards to ensure proper rest and equitable rotation.

Personnel shall be added from the trained roster as required by this plan. Each active guard is equipped with a radio, flashlight, multitool, PFD and standard Safety Gear. There is no specific uniform to wear however, an identification badge is given to each active guard which states they are facility security. These badges have photos and are worn on to clip on the chest or to hang in a see through pouch.

E. Contact Numbers

Facility Security Officer	##		
Canville Police Emergency	##	Canville Fire	##
Coast Guard COTP	##	State Patrol	##
National Response Center	800-424-8802	or	202-267-2675
FBI Local Agent	##		

Facility Security Plan//Sensitive Security Information

Section 2 Personnel Training

A. Record Keeping

The training records for facility personnel are kept in the Facility Security Officers' Office in the main building (Number 212) on the Howie Bay site. These files are kept electronically and in paper form. All training and other records stay in the FSO Office and may not be removed. This is a locked space and shall not be open and unattended.

B. Training Requirements

Facility Security Officer: The following courses (or equivalents) are required of the person who will act as Facility Security Officer. (The position of FSO requires a minimum of B.S. in Industrial Systems or equivalent technical and on the job training prior to being hired)

1. FEMA Response to Emergencies
2. Clean Coast ICS Introductory Course
3. Clean Coast ICS Advanced Course
4. Train the Trainer: Intro to ICS by CC Response Systems
5. Canville College Physical Security Systems
6. Spill Response Course TX A&M
7. Maritime Law Introductory Course at Canville College
8. Risk Management Techniques at Canville College

In addition:

1. The FSO must have completed the Tankerman's Course at Phil's Maritime Academy and may apply for a tankerman's card through the CG by following Company Policy of advanced education (contact Zoe Mutzert at 4451).
2. The FSO shall spend two weeks in on the job training at each station, ships, barges, trucks, rail cars and fishing boats.

Patrol Team One: Shall be hired from personnel with law enforcement backgrounds, as available. Where not available personnel with an academic training of the Associates Level or higher shall be considered. After the prerequisites have been met the following courses are required:

1. FEMA Response to Emergencies
2. Introductory ICS Course (provided by the FSO)

In addition, personnel from Patrol Team One shall be members of each existing section, Ships, Barges, etc. They will be responsible for teaching basic security awareness to their fellow employees. Membership in Patrol Team One is a privilege, with this responsibility comes a bonus, computed monthly and dependent of performance in actual events, drills and exercises.

Section 3 Drills and Exercises

A. Drills

The Facility Security Officer shall initiate a drill at any time desired at a minimum this shall occur once every other month. The drill will test a small section of the overall response to a Security Incident. Records shall be kept in the Facility Security Officers files. **Official regulations call for a drill every three months.** Our facility will incorporate the monthly drill schedule instead, though on months with an exercise no drill will be required.

Examples of routine drills are:

1. Unauthorized person tries to gain access to the facility through a shoreside gate. This is to test the first person on scene and to check that notification gets all the way to the FSO
2. Recreational Boater ties up to barge dock and wanders on to the facility. Test awareness of all personnel and notification chain again.
3. Problem aboard a ship. Test notification chain and time to put Patrol Team One into position.

B. Exercises

Exercises will be arranged by FSO to test all the elements of the plan. It is desirable to invite in some personnel who are sufficiently trained and not threats to SSI to assist in this endeavor. Big Bob's Security Training Team out of Houston, Tennessee was invited in 2002 for an exercise in security. Bog Bob's is a John Doe Company. It may be possible to get involvement from Federal and State entities for these exercises as well. Prior to beginning the exercise it will be made abundantly clear whether it is a tabletop exercise or a physical deployment exercise. **Exercises will take place once each calendar year, with no more than 18 months between begin dates.**

Examples of scenarios:

1. Protesters turn nasty and attempt sabotage.
2. Foreign Vessel Crew becomes violent.
3. Drunken Fishermen begin a brawl.

Section 4 Records and Documentation

All records required by regulation will be kept in the Facility Security Officer's Office. This space is secured by a keypad lock system. Inside a monitored building, with no external windows. The computer files shall be kept on a standalone computer without access to the internet and password protected to the FSO, Assistant FSO and General Manager. Passwords will change when personnel change or every sixty days.

There will be locked filing cabinets for paper copies of all records. These documents will be marked as required by SSI and proprietary regulatory measures. Training records, drill records and exercise records will be made available to company personnel as required to assist in keeping training up to date. A persons training file shall be shredded one year after they have left company employment. The electronic copy shall be maintained for ten years. All other paper records will be shredded five years after use is completed and an electronic copy kept indefinitely. **Current regulations call for all records detailed in this section to be kept for two years. The electronic copies fulfill this requirement and regs allow for electronic filing.**

Records of changes in MARSEC and responses to this and MARSEC Directives shall be kept in a separate system with release carefully regulated. This information will be the most useful in developing updates to the plan.

Audits, changes and required amendments shall be filed separately in the Administrative files of the FSO for review prior to addition to the plan. They will be released as part of the plan only.

Declaration of Security paperwork shall have a separate drawer and shall be released only at the FSO/Vessel Security Officer level or when absolutely required. These Documents shall be kept a minimum of 90 days after the vessel has departed the dock.

The records of the security equipment, including inventory, maintenance, calibration, operating manuals, repair and failure records shall be kept in a separate filing cabinet in the FSO Office. These records will not be maintained electronically. It is the FSO's responsibility to ensure that the technicians keep these records up to date. Records will be kept until the equipment is removed from service and discarded.

Section 5 Response to a Change in MARSEC

This plan has specific items, detailed in later sections, for responding to increases in MARSEC level. At each step up security increases. Patrol Team One and the Facility Security Officer Trained persons can provide twelve hour watch sections for approximately two weeks before fatigue will require new personnel. This is for a worst case scenario of actual attacks in the area with a threat of an explosive or other deadly threat to the facility confirmed.

For MARSEC 1 there are two personnel required and the FSO carries a beeper and can be on site within two hours. As the facility has comfortable on site living quarters then as MARSEC increases people will be brought in and kept on site. There is a kitchen facility which can be stocked as needed.

When MARSEC is reduced personnel will be released as soon as is practical. However, it is good practice to get input from personnel on their perception of the response in the form of critiques if possible before they are released.

It is believed that by following the procedures in this plan increases in the security measures required by increases in MARSEC can be rapidly implemented. When MARSEC decreases it should be possible to release personnel at the ends of watch shifts and still function quite well.

Unfortunately, personnel serving the MARSEC Security role are being pulled from routine functions in other segments of the facility operation. They will need to be allowed to rest prior to returning them to their ordinary duties. Personnel not normally assigned security duties will be impacted by this need to shift personnel resources.

A shift up in MARSEC must be completed within twelve hours. The FSO utilizing the Patrol Group One employees shall ensure that all company personnel are aware of a change in security level. The FSO is responsible for keeping in touch with the Coast Guard and informing of

Section 6 Procedures for Interfacing with Vessels

Reference other sections of the plan as appropriate. The security on the vessel and the facility should be coordinated. Points of Contact that are valid for the entire stay of the vessel must be identified. A communication system of cell phones or radios or both shall be identified, tested and used.

Considerations include:

- Access Vessel personnel to the facility for non transfer related activities.
- Access of Vessel personnel to the facility for transfer related activities.
- A list of personnel on board the vessel who may act in a security role.
- Notification procedures for the vessel in case of emergency.
- Notify the vessel of any Coast Guard restrictions on the waters, like Security Zones.

Standard Declaration of Inspection and Operations Procedures shall apply as well as necessary security precautions while the vessel is moored and transferring.

When barges or fishing vessels are moored additional security shall be set for these vessels as required to ensure the safety of the facility. It will be carefully considered whether the fishing vessel refueling section shall shut down at MARSEC III.

A checklist in the style of a Declaration of Inspection is in review by company officials. This will make the first change when it is completed. Until the time it becomes current then make sure the comms have been tested. That there is an English speaking contact on duty during each watch and add the considerations above to the Declaration of Inspection check off in the remarks section.

Section 7 Declaration of Security

At MARSEC Level one this facility is not called on to make a formal Declaration of Security. Instead, we will follow the requirements of the previous section. There shall be methods in –place to clearly communicate security concerns and some generic information as well.

At MARSEC Level II the following items shall be considered and a written agreement executed:

1. Roving Guards on the dock, time between rounds.
2. Roving Guards on the vessel, time between rounds.
3. Test for communications system, time between tests.
4. Physical survey of connections, including mooring lines.
5. Waterside surveillance and passing information on contacts.
6. Notification chain in case of incident tested, on what time table.
7. Identifying checkpoints and manning them at access way to the vessel.

At MARSEC Level III the following additional items will be instituted.

1. Small boat launched for patrol, schedule determined by environment
2. Additional roving patrols or decreasing the time between patrols.

Facility Security Plan//Sensitive Security Information

Section 8 Communications

A. Physical Communications Systems

This facility will use Moterella PH12 hand held intrinsically safe radios as the primary communications on the facility. We have procured simple scrambling systems for these radios and a base station for the main guard shack. Preset channels 1, 2, and 3 have been programmed with frequencies, which are appropriate, and legal as set by FCC. Licenses for these channels are held in the FSO Office and copies are maintained at the guard shack and the Admin Desk. The radios will be issued from the guard shack, which is manned 24 hours a day and seven days a week. These radios have a range of twelve miles from the facility. Problems should be entered in the Radio Equipment Log. Emergency procurement of radios or repair shall be forwarded through the on duty senior guard and notification made to the FSO.

There are limited intercoms on the facility. An up to date list of what extensions are where shall be kept at each telephone or intercom. The intercoms are non secure but isolated and can be used for internal response to incidents.

Specific personnel have been issued cellular phones. Contact of these persons using those numbers should be limited to notification. Full incident briefs should be on landline, which is safer from casual listeners. Keep information of a security nature off cellular phones. Request contact by secure radio or landline before releasing information that could endanger persons, property or security organization (like computer passwords or MARSEC Directives).

B. Communications in General

Don't spread information unless there is need. Keep you radios charged. Test intercoms and telephones as part of standard procedures to ensure the accuracy of the telephone directory. Report missing, damaged or malfunctioning equipment to the Guard Shack.

There is a requirement to pass some information however, and to inform to an appropriate degree every employee as to the security condition current on the facility. This process is initiated by the FSO. Near the front gate Guard Shack is the Facility Notice Board. Everyone coming onto our facility has seen it because it was placed to be obvious. Usually it states “## of days since the last injury” and the time of the next labor organization meeting. Well the current Security Warning will be placed there in this format: “Security is Job One” at MARSEC I. If MARSEC levels change the message will become “Contact your member of Security Patrol One today”.

The FSO will call the members of Security Patrol One as part of the change of MARSEC condition (in either direction). Then it is their responsibility to pass this to the people in their shops, that security concerns have increased or decreased and specifics on what to be on the look out for, from small boats with protestors to people trying to hitch a ride on the rail cars.

Section 9 Security Systems and Equipment Maintenance

A. Physical Systems

Fencing around the facility is ten foot chain link with three lines of barbed wire angled at the top for all landward perimeters. There are four gates, two for rail and two for vehicles. The Fishing vessel segment is cut off from the Main facility grounds by eight foot chain link and there is a gate there as well. The water side perimeter is with the exception of the docking areas is fenced in a similar manner at the high tide line. In the vicinity of the docks fences are reduced to eight feet without barbed wire. There are gates which allow access at the mooring areas. When vessels are in it is required that facility personnel be in the transfer shacks. SLK is not a permanent mooring facility. There is a fishing vessel harbor five miles south in Fuiliett. Mooring is for transfer purposes only.

Each docking area has a camera. Digi 400 System provides these security cameras, the monitors are in the guard shack and feeders in the FSO Office. Digi 400 provides preventive maintenance and has a 24 hour emergency maintenance contract with SLK. Contact the Guard Shack or the FSO if problems arise.

Radios are maintained as listed previously. The facility guard has a Hondo ATV (six wheeled) to do routine rounds (two seater). The Hondo is maintained by the SLK garage. There is a response kit with emergency lights, bullhorn and toolkit which is also maintained by the garage. A log and inventory is kept by the garage mechanic and turned in to the FSO monthly.

The gates at the mooring areas and the rail will be secured with chains and locks when not in use. The vehicle main gate, and fishing vessel gates are controlled by the guard shack and entry is granted after calling in on the intercom or by entering a pass code on a keypad at the gate.

The lighting on the facility is divided into the perimeter lights which are forty feet high and placed every 100 feet. These are three fixture, high candle, white lights. Two of the fixtures operate under normal conditions and one is run when the emergency generator is on. Then there are the normal facility light fixtures which are detailed in the electricians shop wiring diagrams. All problems with the lights should be routed through the electrician. For emergency service the FSO has a 24 hour contact with a local company to provide portable lights.

B. Electronic Systems

The computer systems on the facility are protected by HOTshots Security Programs. This is the latest in tech support from our IT contractor SiimiCen. A physical and electronic firewall is installed through the computer system center at the Admin Desk. For normal problems contact the sysman via email or phone (see directory). After hours and with non routine problems, call tech support. They are available all day every day at a number listed at the bottom of the phone extensions card located at every phone.

Facility Security Plan//Sensitive Security Information

The FSO computer is a standalone and SHALL not be connected to internet service. There will be a separate compute in the FSO Office for normal work, which requires internet access.

Section 10 Security Measures for Access Control

MARSEC I

1. Two Guards shall be on duty at all times. These are members of Patrol Team One. One will remain in the guard shack and monitor radio, phone and cameras.
2. The vehicle gates will be opened only after the duty guard is contacted.
3. If the gate is opened by passcode the on duty guard will make a notation in his/her Daylog.
4. Rounds shall be conducted once every three hours.
5. Oversight by dock men and such shall be entered in the Daylog. It is company policy that a member of the specific shop be on scene as facility contact for transfers (see Operations Manuals for each Facility Shop)

MARSEC II

1. Four Guards shall be on duty at all times, and the FSO shall be on site for the duration of any vessel operation.
2. Both guard shacks shall manned.
3. Roving patrols every two hours.

MARSEC III

1. Five Guards and the FSO shall be on scene if any operation is in progress.
2. The keypad shall be disabled and all visitors checked for proper ID before entry to the facility is granted.
3. No fishing vessel refueling will take place.
4. During daylight hours properly trained Patrol Group One personnel in the Oil Response 17 foot motorboat will make a boat patrol, if a deep draft vessel is moored to the facility.
5. A comms check and Daylog entry shall be made every thirty minutes.

Facility Security Plan//Sensitive Security Information

Section 11 Security Measures for Restricted Areas

A. Designated Restricted Areas

The entire facility, SLK Fueling and Distributing has been designated a restricted area in accordance with the regulatory definition in 33 CFR 105. The exterior fences have metal signs every fifty feet with the following marking in 4 inch letters:

RESTRICTED AREA

Authorized Personnel Only

Violators are subject to prosecution.

Also, the facility board at the main gate has this message in eight inch letters, and each gate has the message in two inch lettering on metal signs.

B. MARSEC I

Authorized personnel only, each person doing business with the facility will be identified and logged. Only employees may move beyond the immediate transfer sites without permission by the guards. All other MARSEC I conditions in this manual apply as the entire facility is restricted. As levels increase the following items shall be added.

C. MARSEC II

1. Closure of sections of the facility, the fishing vessel moorage shall be contemplated.
2. Each customer, contractor or other authorized visitor will be accompanied by a facility employee.
3. Visitor badges shall be counted every half hour and the location of each visitor confirmed.

D. MARSEC III

1. Closure of the fishing vessel moorage shall take place. Transfers will discontinue and any moored vessels shall depart within two hours.
2. The rear gate and both rail gates shall be chained and locked shut.
3. The gates to the docks at the fishing vessel moorage shall be chained and locked.
4. The transfer manifolds shall be isolated and locked and the valve in the tank farm shall be secured.
5. No more than one barge or one deep draft vessel will be allowed moored to the facility at the same time.

Section 12 Security Measures for Handling Cargo

MARSEC I

1. Follow standard procedures as printed in the CG Approved Operations Manual.
2. Guard on standard rounds shall confirm that the PIC for the facility and for the vessel are awake and aware.

MARSEC II

1. Add personnel at the tank farm to gauge and sample cargo delivered at 1.5 the rate required by our standard operating procedures.
2. If possible put two PICs on each transfer.

MARSEC III

Two PICs shall be present at any transfer.

The FSO shall review procedures and hook up before any transfer starts.

Section 13 Security Measures for the delivery of vessel stores and bunkers

MARSEC I

This section applies only to the deliveries to the deep draft vessels. Fuel, bunkers and lube oils are delivered as per the cargo transfer section (previous section).

Vessel stores shall be delivered from the shoreside. There is neither the room nor the safe maneuvering space for a barge to pull outboard of the ships at the deep draft moorage. There may be arrangements for delivery of food, paints, or motor parts. There may be arrangements for the disposal of garbage as well. Our facility can and does arrange for oil waste to be removed and has a contract for garbage removal (note that the facility holds Certificates of Adequacy for oil and trash). Any deliveries or waste removals must be scheduled at the time that advance notice of arrival is confirmed, which is 96 hours before arrival at the dock. This is the minimum time allowance that can be accommodated.

Any delivery that arrives at the gate that has not been scheduled SHALL be turned back. The VSO and the FSO may make arrangements to have a delivery after the ship arrives if there are unusual circumstances that require deviation from this policy.

All delivery trucks will be stopped at the gate. The packing slips and delivery order will be checked. The guards will confirm the order with the FSO and ship point of contact. The driver of the truck shall be logged in and his/her license checked.

MARSEC II

1. There shall be no exceptions to the arrival notice for delivery of vessel stores.
2. Removal of wastes may be conducted if the circumstances warrant.
3. A physical search of the truck to confirm each parcel.
4. A phone call to the shipping company office to confirm that this truck is a valid carrier.
5. A facility representative will ride with the truck or the guard vehicle will escort to the dock and back after offload is completed.

MARSEC III

1. There will only be stores delivered if 120 hour notice is given.
2. The company delivering the parcel shall contact the FSO with name of the driver.
3. The FSO will be contacted before allowing the truck to enter the facility.
4. The FSO or a Patrol Team One member will stay with the truck the entire time it is on the facility.

Section 14 Security Measures for Monitoring

MARSEC I

Monitoring of the facility is first and foremost among the jobs that the guards are responsible to complete. They have at their disposal remote cameras, intercoms to communicate with other inhabitants and a patrol vehicle. In the vehicle are binoculars and the FSO is planning on procuring night vision glasses of the light amplifying type.

Every three hours:

1. Patrols shall inspect the perimeter fence.
2. Check locked and chained gates.
3. Ensure all perimeter lights are working (night only).
4. Survey actions at the transfer areas.
5. Confirm radio operations by calling in every fifteen minutes.

MARSEC II

1. The patrols shall become more frequent.
2. At each camera the mobile guard shall confirm proper operation.

MARSEC III

1. Perimeter patrols shall be hourly, which is nearly continuous as a routine patrol is currently gauged at fifty minutes.
2. An additional ATV will be brought out of the motor pool.
3. A foot patrol of the main facility grounds will take place every four hours.
4. A small boat will be launched to patrol as detailed earlier in this plan.

Section 15 Security Incident Procedures

Should an incident occur it is important that all employees take the fastest course to safety. We have drilled on oil spill response previously and how non essential or untrained personnel should leave the area.

It should be the instinct of each employee to evacuate to the fire safety area as defined by their shop and follow personnel accountability procedures. This will help us discover any missing persons. The evacuation alarm for fire and security are identical. Members of Patrol Team One will be activated and know if an incident has occurred. Radio's issued from the guard shack are to be the primary communication method. Should evacuation to the secondary site outside the gates guards will be indicating the path.

The FSO shall gather all pertinent details of the incident that are initially available and make first notifications to cognizant authorities and emergency responders who can help with the situation. It is highly likely that outside personnel will arrive and the coordination of a response will lie with the FSO. The FSO will use ICS as the tool for organizing the response.

If an evacuation is not called for the FSO shall direct Patrol Team One personnel to sections of the facility to stop or stabilize operations that may be threatened. All affected personnel must know what is happening.

Section 16 Audits and Amendments

A. Audits

The plan shall be audited each year in the same month that the plan was approved. The plan shall be audited if a new FSO is employed. The plan shall be audited if ownership of the facility changes or major modifications are made.

Audits shall be conducted by Stable Security Consultants, a nationally accredited firm.

B. Amendments

If the facility changes significantly, the operations change, personnel change and in certain other conditions an amendment may be required. These amendments are made by the FSO and submitted to the cognizant COTP for approval.

Section 17 Facility Security Assessment Report

This section is held for a report by Farsight Security Consultants who have surveyed our facility on three occasions. Their report is not to be released to anyone not needing to see it, it is perhaps the most sensitive information in the plan. This multipage document was a labor for the consultant and the FSO.

The regulations call for a security assessment to be accomplished using the guidelines of 33 CFR 105.300 all.

Section 18 Facility Vulnerability and Security Measures Summary

See attached document CG-6025

“WARNING: THIS DOCUMENT CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER THE PROVISIONS OF 49 CFR PART 1520. NO PART OF THIS DOCUMENT MAY BE RELEASED WITHOUT THE WRITTEN PERMISSION OF THE UNDER SECRETARY OF TRANSPORTATION FOR SECURITY, WASHINGTON, D.C 20590. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION. FOR US GOVERNMENT AGENCIES, PUBLIC AVAILABILITY TO BE DETERMINED UNDER 5 U.S.C. 552.”